STATE OF CALIFORNIA

Budget Change Proposal - Cover Sheet

DF-46 (REV 08/15)

Fiscal Year 2016-17	Business Unit 7501	Department HUMAN RESOURCES	Priority No. 2

Budget Request Name 7501-006-BCP-2016-BR-GB	Program **9900100/9900200**	Subprogram

Budget Request Description
Information Security Staffing

Budget Request Summary

This proposal requests one permanent position and $154,000 ($19,000 General Fund, $11,000 Central Service Cost Recovery Fund, $25,000 Deferred Compensation Plan Fund, $99,000 Reimbursements) in fiscal year 2016-17 and $145,000 ($17,000 General Fund, $10,000 Central Service Cost Recovery Fund, $24,000 Deferred Compensation Plan Fund, $94,000 Reimbursements) in fiscal year 2017-18 and ongoing to address workload resulting from security assessments and the need to improve security practices in the department.

Requires Legislation □ Yes ☒ No	Code Section(s) to be Added/Amended/Repealed	
Does this BCP contain information technology (IT) components? ☒ Yes □ No *If yes, departmental Chief Information Officer must sign.*	Department CIO Chad Crowe	Date 12/29/15

For IT requests, specify the date a Special Project Report (SPR) or Feasibility Study Report (FSR) was approved by the Department of Technology, or previously by the Department of Finance.

□ FSR □ SPR Project No. Date:

If proposal affects another department, does other department concur with proposal? □ Yes ☒ No
Attach comments of affected department, signed and dated by the department director or designee.

Prepared By Victor Mendoza	Date 12/29/2015	Reviewed By Chad Crowe	Date 12/29/15
Department Director Richard Gillihan	Date 12/29/15	Agency Secretary Marybel Batjer	Date 12/3/15

Department of Finance Use Only

Additional Review: □ Capital Outlay □ ITCU □ FSCU □ OSAE □ CALSTARS □ Dept. of Technology

BCP Type: □ Policy ☒ Workload Budget per Government Code 13308.05

PPBA	Date submitted to the Legislature 1/7/16

BCP Fiscal Detail Sheet

BCP Title: Information Security Staffing

DP Name: 7501-006-BCP-DP-2016-GB

Budget Request Summary			FY16			
	CY	**BY**	**BY+1**	**BY+2**	**BY+3**	**BY+4**
Positions - Permanent	0.0	1.0	1.0	1.0	1.0	1.0
Total Positions	**0.0**	**1.0**	**1.0**	**1.0**	**1.0**	**1.0**
Salaries and Wages						
Earnings - Permanent	0	89	89	89	89	89
Total Salaries and Wages	**$0**	**$89**	**$89**	**$89**	**$89**	**$89**
Total Staff Benefits	0	44	44	44	44	44
Total Personal Services	**$0**	**$133**	**$133**	**$133**	**$133**	**$133**
Operating Expenses and Equipment						
5301 - General Expense	0	3	3	3	3	3
5302 - Printing	0	1	1	1	1	1
5304 - Communications	0	1	1	1	1	1
5320 - Travel: In-State	0	2	2	2	2	2
5322 - Training	0	4	4	4	4	4
5324 - Facilities Operation	0	7	0	0	0	0
5346 - Information Technology	0	3	1	1	1	1
Total Operating Expenses and Equipment	**$0**	**$21**	**$12**	**$12**	**$12**	**$12**
Total Budget Request	**$0**	**$154**	**$145**	**$145**	**$145**	**$145**
Fund Summary						
Fund Source - State Operations						
0001 - General Fund	0	19	17	17	17	17
0915 - Deferred Compensation Plan Fund	0	25	24	24	24	24
9740 - Central Service Cost Recovery Fund	0	11	10	10	10	10
0995 - Reimbursements	0	99	94	94	94	94
Total State Operations Expenditures	**$0**	**$154**	**$145**	**$145**	**$145**	**$145**
Total All Funds	**$0**	**$154**	**$145**	**$145**	**$145**	**$145**
Program Summary						
Program Funding						
6200 - Human Resources Management	0	85	81	81	81	81
6210 - Benefits Administration	0	48	45	45	45	45
9900100 - Administration	0	154	145	145	145	145
9900200 - Administration - Distributed	0	-133	-126	-126	-126	-126
Total All Programs	**$0**	**$154**	**$145**	**$145**	**$145**	**$145**

Personal Services Details

	Salary Information								
Positions	Min	Mid	Max	CY	BY	BY+1	BY+2	BY+3	BY+4
1367 - Sys Software Spec III (Tech) (Eff. 07-01-				0.0	1.0	1.0	1.0	1.0	1.0
Total Positions				**0.0**	**1.0**	**1.0**	**1.0**	**1.0**	**1.0**

Salaries and Wages	CY	BY	BY+1	BY+2	BY+3	BY+4
1367 - Sys Software Spec III (Tech) (Eff. 07-01-	0	89	89	89	89	89
Total Salaries and Wages	**$0**	**$89**	**$89**	**$89**	**$89**	**$89**
Staff Benefits						
5150210 - Disability Leave - Nonindustrial	0	1	1	1	1	1
5150350 - Health Insurance	0	13	13	13	13	13
5150450 - Medicare Taxation	0	1	1	1	1	1
5150500 - OASDI	0	6	6	6	6	6
5150600 - Retirement - General	0	22	22	22	22	22
5150800 - Workers' Compensation	0	1	1	1	1	1
Total Staff Benefits	**$0**	**$44**	**$44**	**$44**	**$44**	**$44**
Total Personal Services	**$0**	**$133**	**$133**	**$133**	**$133**	**$133**

Analysis of Problem

A. Budget Request Summary

This proposal requests one permanent position and $154,000 ($19,000 General Fund, $11,000 Central Service Cost Recovery Fund, $25,000 Deferred Compensation Plan Fund, $99,000 Reimbursements) in fiscal year 2016-17 and $145,000 ($17,000 General Fund, $10,000 Central Service Cost Recovery Fund, $24,000 Deferred Compensation Plan Fund, $94,000 Reimbursements) in fiscal year 2017-18 and ongoing to address workload resulting from security assessments and the need to improve security practices in the department.

B. Background/History

The Information Technology Division (ITD) within the Department of Human Resources (CalHR) has the responsibility of providing information technology services for both CalHR and the State Personnel Board (SPB). ITD maintains web sites, applications and sensitive and confidential data sets that serve state departments, state employees, and the public.

ITD provides CalHR and SPB business units with enterprise support for Wide Area Network (WAN)/Local Area Network (LAN) connectivity, servers, desktops, messaging, and mainframe services. ITD is responsible for software development including web development and client/server application implementations and providing technical support for the hardware, system software layer and application layer for all hardware and software systems on the CalHR network. This includes Active Directory, Exchange, document management, content management, routers, switches, firewalls, servers and Storage Area Network. In addition, ITD configures and maintains all CalHR and SPB web servers and websites; coordinates and supports decentralized content authors as well as establishes and publishes standard procedures and technology for these environments.

ITD works towards the implementation of new technologies designed to meet the ever-growing demands of external stakeholders and its business partners within CalHR and SPB. ITD works to enhance and support applications that are specific to both CalHR and SPB as well as several statewide applications, including the Statewide Examination and Certification Systems, Statewide/Departmental Internet Examinations, Examination Bulletin System, Vacancy Position Database, HRNet, and the Layoff Application. CalHR is responsible for the Examination and Certification Online System (ECOS) Project, designed to replace the state's existing Examination and Certification Systems. ECOS is expected to be completed by July 2017.

ITD provides indirect support to external trusted business partners (personnel officers, budget officers, and finance personnel) through the use of IT-supported systems to collaborate, access reports and documents, perform transactions, and manage workflow. In addition, ITD maintains 70 secured electronic interfaces between the State Controller's Office, third-party administrators, unions, and other entities the department conducts business with. Millions of dollars in transactions associated with the Savings Plus program are supported by this infrastructure. The Savings Plus program is the 401(k) Plan and 457 Plan available to state and California State University employees.

ITD provides support and maintenance to SPB applications including, Appeals Case Tracking System, Kwikwork/FileNet, Legal Case Tracking System, and TeamMate Audit Management System.

ITD is responsible for planning, oversight, and coordination of CalHR and SPB information security program activities to effectively manage risk, provide for the protection of information assets, and prevent illegal activity, fraud, waste, and abuse in the use of information assets in accordance with State Administrative Manual (SAM) Section 5300 and State Information Management Manual (SIMM) 5305-A. These manual sections are the state policies and standards for information security. Through recent assessments, we have become aware that ITD needs additional assistance to keep CalHR and SPB in compliance with SAM 5300 and SIMM 5305-A, putting CalHR and SPB at risk of a potential security breach.

C. State Level Considerations

The State of California runs a significant risk of liability if there were to be sensitive data loss and/or continues to have an inaccessible web presence. ITD handles sensitive data for all state employees. If there were a data breach, the state would be responsible for notifying those affected by the breach. This could result in potential costs to the state in terms of exposure to litigation and other costs that would be a consequence of a security breach. The amount of liability varies depending on the amount of data that is breached and could range from hundreds to millions of dollars.

All departments, state employees, and the public interact with CalHR and SPB applications, data sets, and websites. The jobs.ca.gov site created and maintained by CalHR, produces a large amount of traffic as it is one the top sites visited in California government. This added exposure increases security risks.

D. Justification

ITD does not have a full-time Information Security Officer (ISO). As a result of security assessments, it has become evident that CalHR needs additional assistance in maintaining the proper and effective documentation, policies, procedures, or unbiased internal checks. CalHR handles several data sets that are considered sensitive. CalHR must be diligent in providing the proper level of security monitoring and be actively engaged in security activities. As the State ISO details in the SIMM 5305-A, the ISO is responsible for:

1. Management and oversight of the state entity's Information Security Program ensuring protection of the state entity's information assets and state entity compliance with state information security policies, standards, and procedures. These include, but are not limited to, the following areas:

   - Risk Management
   - Policy Management
   - Organizing Information Security
   - Asset Protection
   - Human Resource Security
   - Physical and Environmental Security
   - Communication and Operations Management
   - Access Control
   - Information Systems Acquisition, Development, and Maintenance
   - Incident Management
   - Disaster Recovery Management
   - Compliance with state information security policies, standards, and procedures

2. Possessing the qualifications (education, training, skills, and knowledge) sufficient to effectively execute the duties and responsibilities of the position.

The workload involved with ensuring security compliance requires a dedicated ISO as per the recommendation of California's State ISO. Today, CalHR has a part-time ISO that is split between three different areas, these are: 1) serves as the department's lone quality assurance tester for all websites and software applications; 2) serves as the department's privacy program manager, which is also recommended to be a dedicated position; and 3) serves as the department's ISO.

In a recent review of CalHR's web sites for accessibility, it was noted that CalHR was not in compliance with accessibility mandates and we do not have the proper processes and procedures in place to maintain this kind of compliance. The additional work involved with getting all of CalHR's web sites in compliance and ensuring they stay in compliance falls on our quality assurance tester. This quality assurance testing workload falls on our current ISO's additional duties. This person does not have the time to establish the security standards set forth by the federal and state governments or maintain them going forward as additional security measures and assessments need to be implemented and at the same time ensure all web sites are accessible. This puts the sensitive data maintained by CalHR at risk as well as the reputation of the department and the state. This kind of risk and exposure could cost the state in damages that could be incurred by a security breach if CalHR does not ensure the proper procedures, documentation and polices. CalHR needs to adhere to these requirements to protect its information assets and secure the sensitive data that CalHR possess and this cannot be accomplished with current resources.

E. Outcomes and Accountability

The approval of this request will provide the greatest benefit as CalHR will significantly reduce exposure to costs and damages that could be incurred by a security breach while enabling CalHR to comply with the SAM 5300 and SIMM 5305-A requirements to protect its information assets and secure the sensitive data gathered. Approval will also allow CalHR to conduct biennial risk assessments, required by SAM 5305.7 and certify risk and privacy program compliance on a yearly basis as required by SIMM 5330-B.

Recent legislation requires that the State Information Security Office assess all departments on a recurring basis. The results of these audits will be made public. Approval of this request will allow CalHR to remediate issues found by the audit in a timely manner and maintain security compliance as technology changes. Recent policy changes require that on a quarterly basis CalHR report security issues to the California Information Security Office. Approval of this request will allow CalHR to accurately report security issues.

F. Analysis of All Feasible Alternatives

Alternative 1: Approve Request
Pro: CalHR will be able to address the additional workload resulting from recent security assessments and will ensure that CalHR will be in compliance with security standards going forward. A dedicated ISO will significantly reduce exposure to costs and damages that could be incurred by a security breach while enabling CalHR to comply with the SAM 5300 and SIMM 5305-A requirements to protect its information assets and secure the personal information gathered from candidates and employees.

Con: There would be an increased cost to the state and an increase to the state workforce.

Alternative 2: Approve One Year Limited Term Position
Pro: CalHR will be able to address some of its security issues from the recent security assessments. The cost to implement this is less than Alternative 1.

Con: CalHR will not be able to address all issues from the security assessment and therefore will be out of compliance with SAM 5300 and SIMM 5305-A requirements. CalHR will not have the ability to maintain security compliance, which could result in potential cost to the state in terms of exposure to litigation and costs that would be a consequence of a security breach.

Alternative 3: Do not approve this request
Pro: There would be no cost to the state and no growth to the state workforce.

Con: This alternative has a potential cost to the state in terms of exposure to litigation and costs that would be a consequence of a security breach.

G. Implementation Plan

Task	Due	Responsibility
Recruit	May 2016	CIO
Hire	July 2016	CIO
Setup standards, process, procedures and policies to ensure CalHR and SPB are in compliance with SAM 5300 and SIMM 5305-A	January 2017	ISO
Ensure CalHR and SPB are in compliance with SAM 5300 and SIMM 5305-A	July 2017	ISO

H. Supplemental Information

See attached Workload Matrix.

I. Recommendation

Approve Alternative 1. This will allow CalHR to add a permanent full-time ISO to mitigate potential security risks and ensure that CalHR and SPB are in compliance with SAM 5300.

DEPARTMENT OF HUMAN RESOURCES
2016-2017 BUDGET YEAR
BUDGET CHANGE PROPOSAL
WORKLOAD MATRIX

DIVISION: Information Technology Division
POSITION TITLE: Systems Software Specialist III (Technical)

Position(s) Requested	Workload	Workload Standard	Basis for Standard
Systems Software Specialist III (Technical): 1.0	**Year One**		
	Task #1 Establish Policy: Establishing standards, process, procedures, and policies to ensure CalHR and SPB are in compliance with SAM 5300 and SIMM 5303-A.	**Hours: 525**	Assumes initial baseline controls for a moderate level system as defined by the National Institute of Standards and Technology which is over 150 controls that need to be developed. 150 x 3.5 hours per control = 525 hours
	Task #2 Risk and Security Assessment of Applications: Conduct risk and security assessment of all applications against established policies.	**Hours: 1,000**	50 systems x 20 hours per assessment =1,000
	Task #3 Organizational Risk Assessment: Conduct risk assessment at organization and division level.	**Hours: 238**	14 Divisions x 17 hours per assessment = 238
		Total Hours: 1,763	
	Ongoing		
	Task #1 Security Assessments and Risk Management: Participate in the assessment, evaluation, and documentation of life-cycle needs for security technology systems and provide	**Hours: 710**	

	recommendations for improvement. Conduct ongoing risk assessments.		
	Task #2 Monitor Systems: Perform continuing compliance monitoring of the information security posture via security tools to ensure security compliance. Responsibility for ensuring that CalHR's and SPB's security technology tools and systems are functioning effectively and efficiently.	**Hours: 710**	
	Task #3 Maintain Policies: Maintain standards, processes, procedures, and policies to ensure CalHR and SPB are in compliance with SAM 5300 and SIMM 5303-A.	**Hours: 178**	
	Task #4 Security Training and Reporting: Creating an information security awareness program to ensure staff members across the organization understand the trade-off between risk and return. Reporting security performance against established security metrics. Protecting data privacy and information integrity in response to business needs and compliance requirements.	**Hours: 89**	
	Task #5 Incident Response Activities: The Department's initial response to a security breach or other incident. The securing of evidence. Implementing measures to prevent further damage. Working with responsible legal, regulatory and government authorities.	**Hours: 89** **Total Hours: 1,776**	